

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-326696
 (43)Date of publication of application : 22.11.2001

(51)Int.Cl. H04L 12/66
 G06F 13/00
 H04L 12/46
 H04L 12/28
 H04L 12/56

(21)Application number : 2000-146598

(71)Applicant : NEC CORP

(22)Date of filing : 18.05.2000

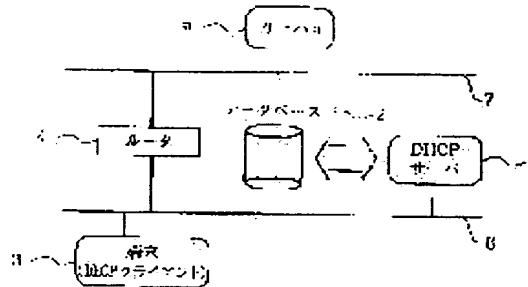
(72)Inventor : KASHIMA KENICHI

(54) METHOD FOR CONTROLLING ACCESS

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an access control method to a server in the unit of users by utilizing a DHCP in a network consisting of terminals connected to a sub net and application servers connected to the server via routers.

SOLUTION: When a terminal is connected to a network, the terminal broadcasts connection request information, the server broadcasts a proposal of assigned setting information, the terminal receiving the proposal of the assigned setting information broadcasts request information including information required for authentication, the server receives information required for the authentication and references a database connected to the server to authenticate the terminal. If the authentication is successful, the server requests access control, corresponding to the terminal to the route. The router, receiving the request, executes filtering of a transmission reception packet on the basis of various sets of information included in the request. The router transmits result information to the terminal and to the server, on the basis of the result of filtering of the transmission reception packet, to complete the connection between the terminal and the server.



LEGAL STATUS

[Date of request for examination] 13.04.2001
 [Date of sending the examiner's decision of rejection] 03.03.2004
 [Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
 [Date of final disposal for application]
 [Patent number]
 [Date of registration]
 [Number of appeal against examiner's decision of rejection]
 [Date of requesting appeal against examiner's decision of rejection]
 [Date of extinction of right]

(19)日本国特許庁 (JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2001-326696

(P 2 0 0 1 - 3 2 6 6 9 6 A)

(43)公開日 平成13年11月22日 (2001. 11. 22)

(51) Int. Cl.	識別記号	F I	テーマコード	(参考)
H04L 12/66		G06F 13/00	351	Z 5B089
G06F 13/00	351	H04L 11/20		B 5K030
H04L 12/46		11/00	310	C 5K033
12/28		11/20	102	D
12/56				

審査請求 有 請求項の数 7 O L (全8頁)

(21)出願番号 特願2000-146598 (P 2000-146598)

(22)出願日 平成12年5月18日 (2000. 5. 18)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 鹿島 謙一

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100088328

弁理士 金田 暢之 (外2名)

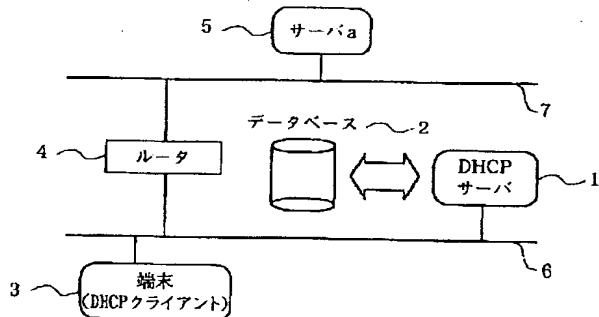
最終頁に続く

(54)【発明の名称】アクセス制御方法

(57)【要約】

【課題】 サブネットに接続されている端末とサーバとルータを介して接続しているアプリケーションサーバから構成されるネットワークでDHCPを利用してユーザ単位でのサーバへのアクセス制御方法を提供する。

【解決手段】 端末がネットワークに接続する際に、接続要求情報をブロードキャストし、サーバが割り当て設定情報の提案をブロードキャストし、割り当て設定情報の提案を受けた端末が認証に要する情報を含む要求情報をブロードキャストし、サーバが認証に要する情報を受け、サーバに接続されているデータベースを参照して認証する。認証に成功すればサーバが端末に対応するアクセス制御をルータに依頼する。依頼を受けたルータは依頼に含まれる各種情報を基に送受パケットのフィルタリングを実施する。ルータは送受パケットのフィルタリングの結果に基づき端末とサーバに結果情報を送信し、端末とサーバの接続を完了する。



【特許請求の範囲】

【請求項 1】 第 1 サブネットに接続されている D H C P クライアント端末と、データベースを持つ D H C P サーバと、第 1 サブネットとルータを介して接続される第 2 サブネットと、第 2 サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、
D H C P を利用し、認証情報データベースによってユーザ単位での前記クライアント端末を認証し、クライアント端末の送受パケットをサーバとルータの連携によってフィルタリングすることを特徴とするアクセス制御方法。

【請求項 2】 第 1 サブネットに接続されている D H C P クライアント端末と、データベースを持つ D H C P サーバと、第 1 サブネットとルータを介して接続される第 2 サブネットと、第 2 サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、
前記クライアント端末が、ネットワークに接続する際に、D H C P サーバから端末認証とユーザ認証を得るステップと、

前記認証によって得られる情報を基に D H C P サーバとルータが連携してユーザ単位のアクセス制御を実施するステップと、

前記認証を得た D H C P クライアント端末のネットワーク接続が完了するステップを有するアクセス制御方法。

【請求項 3】 第 1 サブネットに接続されている D H C P クライアント端末と、データベースを持つ D H C P サーバと、第 1 サブネットとルータを介して接続される第 2 サブネットと、第 2 サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、
前記 D H C P クライアント端末が前記ネットワークに接続する際に、前記 D H C P クライアント端末が接続要求情報をブロードキャストし、前記 D H C P サーバが割り当て設定情報の提案をブロードキャストするステップと、

割り当て設定情報の提案を受けた前記 D H C P クライアント端末が認証に要する情報を含む D H C P 要求情報をブロードキャストし、D H C P サーバが前記 D H C P クライアント端末の認証に要する情報を受け、D H C P サーバに接続されているデータベースを参照して認証するステップと、

認証に成功すれば D H C P サーバが前記 D H C P クライアント端末に対応するアクセス制御をルータに依頼し、認証に失敗すれば前記 D H C P クライアント端末に失敗を報告するステップと、

依頼を受けたルータは依頼に含まれる各種情報を基に送受パケットのフィルタリングを設定するステップと、
前記ルータは送受パケットのフィルタリングの設定結果

に基づき前記 D H C P サーバに結果情報を送信し、さらに前記 D H C P サーバが前記 D H C P クライアント端末に結果情報を返し、最終的に前記 D H C P クライアント端末がネットワーク接続が完了するステップを有するアクセス制御方法。

【請求項 4】 前記送受パケットのフィルタリングを実施するステップが、

前記ルータが、前記 D H C P クライアント端末から送信されるすべてのパケットを受信するステップと、

10 前記ルータが、前記 D H C P サーバで設定されたアクセスリストに基づいて、前記パケットが許可されたものであればアプリケーションサーバに転送し、不許可ならばアプリケーションサーバに転送せずにパケットを廃棄し、履歴としてログ情報を残すフィルタリングステップを有する請求項 1 乃至 3 の何れかに記載のアクセス制御方法。

【請求項 5】 前記第 1 サブネットに接続されている D H C P クライアント端末が、

特別なサブネットマスクを設定して、前記ルータと前記 D H C P クライアント端末のみの第 3 サブネットを形成するステップと、

前記第 1 サブネットに接続されているアプリケーションサーバに前記ルータを介してパケットの送受信を行うステップを有する請求項 1 乃至 4 の何れかに記載のアクセス制御方法。

【請求項 6】 前記第 1 サブネットにさらにエージェント端末を接続し、前記エージェント端末が、
ネットワークに流れる I P および MAC アドレス情報を前記エージェント端末の持つデータベースに収集するステップと、

前記 D H C P サーバが持つ前記 D H C P クライアント端末に関するキャッシュデータと前記エージェント端末のデータベースとを比較検証するステップを有する請求項 1 乃至 4 の何れかに記載のアクセス制御方法。

【請求項 7】 第 1 サブネットに接続されている D H C P クライアント端末と、データベースを持つ D H C P サーバと、第 1 サブネットとルータを介して接続される第 2 サブネットと、第 2 サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、
前記 D H C P クライアント端末毎にアプリケーションサーバへのアクセス制御が行うステップと、

前記 D H C P サーバによるユーザ認証だけではなく、D H C P サーバとルータが連携して、アクセス制御を行うステップと、
前記 D H C P クライアント端末とルータのみのサブネットを構築するステップと、

第 1 サブネットに接続するエージェント端末により不正接続の端末を検出するステップを有することを特徴とするアクセス制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は端末をネットワークに接続する際のアクセス制御方法に関し、特に動的ホスト設定プロトコル (Dynamic Host Configuration Protocol、以降DHCPと称す) を利用するユーザ単位でのサーバへのアクセス制御に関する。

【0002】

【従来の技術】端末をネットワークに接続する際に、DHCPは非常に有用なプロトコルである。しかし、DHCPを使用しても運用面でセキュリティ上に問題点がある。

【0003】

【発明が解決しようとする課題】第1の問題点は、接続要求があれば如何なる端末に対してもインターネットプロトコル (以降、IPと称す) アドレスを割り当て、ネットワークへの接続を許可してしまうということである。その理由は、DHCPには認証の概念が存在しないためである。

【0004】第2の問題点は、運用上ある端末あるいはユーザに対して、特定サーバへのアクセスを拒否したい場合に、それを実現ができないことである。

【0005】DHCPによりIPアドレスを割り当てられた端末は、ネットワークを通じて、WWW、メール、News、プリンタ、ファイルなどのサービスを行っているアプリケーションサーバへアクセスすることが可能となる。もし特定アプリケーションサーバへのアクセスを拒否したい場合には、ネットワークへの接続そのものを拒否する必要があり、ユーザの利便性を著しく損なうことになっている。

【0006】第3の問題点は、何らかの方法で、ネットワークのIPアドレスを不正入手し、手動設定を行うことによりネットワーク接続した場合には、それを防止することができないことである。

【0007】本発明の目的は、以上の問題点を解決するような、サブネットに接続されているDHCPクライアント端末とDHCPサーバとルータを介して接続しているアプリケーションサーバから構成されるネットワークでDHCPを利用してユーザ単位でのアプリケーションサーバへのアクセス制御方法を提供することである。

【0008】

【課題を解決するための手段】本発明のアクセス制御方法は、第1サブネットに接続されているDHCPクライアント端末と、データベースを持つDHCPサーバと、第1サブネットとルータを介して接続される第2サブネットと、第2サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、DHCPを利用し、認証情報データベースによってユーザ単位でのクライアント端末を認

証し、クライアント端末の送受パケットをサーバとルータの協同によってフィルタリングすることを特徴とする。

【0009】また、本発明のアクセス制御方法は、第1サブネットに接続されているDHCPクライアント端末と、データベースを持つDHCPサーバと、第1サブネットとルータを介して接続される第2サブネットと、第2サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、クライアント端末が、ネットワークに接続する際に、DHCPサーバから端末認証とユーザ認証を得るステップと、認証によって得られる情報を基にDHCPサーバとルータが連携してユーザ単位のアクセス制御を実施するステップと、アクセスされたクライアント端末のネットワークへの接続が完了するステップを有する。

【0010】さらに、本発明のアクセス制御方法は、第1サブネットに接続されているDHCPクライアント端末と、データベースを持つDHCPサーバと、第1サブネットとルータを介して接続される第2サブネットと、第2サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法であって、DHCPクライアント端末がネットワークに接続する際に、DHCPクライアント端末が接続要求情報をブロードキャストし、DHCPサーバが割り当て設定情報の提案をブロードキャストするステップと、割り当て設定情報の提案を受けたDHCPクライアント端末が認証に要する情報を含むDHCP要求情報をブロードキャストし、DHCPサーバがDHCPクライアント端末の認証に要する情報を受け、DHCPサーバに接続されているデータベースを参照して認証するステップと、認証に成功すればDHCPサーバがDHCPクライアント端末に対応するアクセス制御をルータに依頼し、認証に失敗すればDHCPクライアント端末に失敗を報告するステップと、依頼を受けたルータは依頼に含まれる各種情報を基に送受パケットのフィルタリングの設定を行うステップと、ルータは送受パケットのフィルタリングの設定結果に基づきDHCPサーバに結果情報を送信し、さらに前記DHCPサーバが前記DHCPクライアント端末に結果情報を返し、最終的に前記DHCPクライアント端末のネットワーク接続が完了するステップを有する。

【0011】また、送受パケットのフィルタリングを実施するステップが、ルータが、DHCPクライアント端末から送信されるすべてのパケットを受信するステップと、ルータが、DHCPサーバで設定されたアクセリストに基づいて、パケットが許可されたものであればアプリケーションサーバに転送し、不許可ならばアプリケーションサーバに転送せずにパケットを廃棄し、履歴としてログ情報を残すフィルタリングステップを有する。

【0012】また、第1サブネットに接続されているD H C P クライアント端末は、特別なサブネットマスクを設定して、ルータとD H C P クライアント端末のみの第3サブネットを形成するステップと、第1サブネットに接続されているアプリケーションサーバにルータを介してパケットの送受信を行うステップを有する。

【0013】また、第1サブネットにさらにエージェント端末を接続し、エージェント端末は、ネットワークに流れるIPおよび媒体アクセス制御（以下MACと称す）アドレス情報をエージェント端末の持つデータベースに収集するステップと、D H C P サーバが持つD H C P クライアント端末のキャッシュデータとエージェント端末のデータベースとを比較検証するステップを有する。

【0014】さらに、本発明のアクセス制御方法は、第1サブネットに接続されているD H C P クライアント端末と、データベースを持つD H C P サーバと、第1サブネットとルータを介して接続される第2サブネットと、第2サブネットに接続されているアプリケーションサーバから構成されるネットワークにおけるアクセス制御方法において、D H C P クライアント端末毎にアプリケーションサーバへのアクセス制御が行うステップと、D H C P サーバによるユーザ認証だけではなく、D H C P サーバとルータが連携して、アクセス制御を行うステップと、D H C P クライアント端末とルータのみのサブネットを構築するステップと、第1サブネットに接続するエージェント端末により不正接続の端末を検出するステップを有することを特徴とする。

【0015】

【発明の実施の形態】次に本発明の実施の形態について図面を参照して詳細に説明する。

【0016】図1を参照すると、本発明の実施例は、D H C P サーバ1と、データベース2と、端末3（D H C P クライアント）と、ルータ4と、端末3と別のサブネット7上に存在するサーバa5とから構成される。

【0017】D H C P サーバ1は、通常のD H C P サーバに加えて、ユーザ認証用のデータとユーザアクセス制御用のデータを含むデータベース2を有す。D H C P サーバ1は、端末3からの要求に対して認証を行い、ルータ4に対してユーザに対応したアクセス制御を依頼する。

【0018】データベース2は、認証データとキャッシュデータから成る。認証データは、認証に必要なユーザID、パスワード、ユーザに対応したアクセス制御を行うためのアクセリストを含む。アクセリストは、発信元IPアドレス（割り当て予定アドレス）、宛先IPアドレス（各種サーバのIPアドレス、ネットワークアドレス）、発信元ポート番号（任意）、宛先ポート番号（各種サーバのポート番号）などのパラメータを組み合わせて、パケットの転送許可、不許可を記述したもので

ある。

【0019】また、キャッシュデータは、運用中に動的に変化するデータで、ユーザIDとそのユーザに割り当てたIPアドレス、ユーザの使用している端末のMACアドレス（Ethernet（登録商標）アドレス）、IPアドレスを割り当てた時刻、リース時間などを含む。

【0020】端末3は、D H C P サーバ1に対してIPアドレスなどの設定情報の割り当てを要求するとともに、認証を受けるための認証情報を提供する。ルータ4は、D H C P サーバ1からの依頼を受けて、アクセス制御を行う。端末3宛てのパケットは必ずこのルータ4を経由することになる。サーバa5は、WWW、メール、News、ファイル、プリンタなどの種々のサービスを提供している端末を示し、端末3と別サブネット7上に存在する。

【0021】次に、図1及び図2及び図3を参照して本実施例の動作について詳細に説明する。

【0022】まず最初に、端末3がネットワークへ接続する際の、認証手順を含んだIPアドレス割り当ての手順を図2を参照して説明する。

【0023】端末3は、D H C P D I S C O V E R をブロードキャストする（ステップ20）。D H C P D I S C O V E R を受信したD H C P サーバ1は、割り当てるべき設定情報を提案するために、D H C P O F F E R をブロードキャストする（ステップ21）。ここまででは通常のD H C P のフローと同様である。設定情報の提案を受けた端末3は、D H C P R E Q U E S T をD H C P サーバ1へブロードキャストする（ステップ22）。このメッセージには、ユーザID、パスワードオプション（ハッシュ化し不可視化する）が含まれる。

【0024】端末3からユーザID、パスワードを含むD H C P R E Q U E S T を受信したD H C P サーバ1は、端末認証およびユーザ認証を行う（ステップ23）。端末認証は、端末3から送信してきたMACアドレスを検索キーとして、データベース2を参照することによって行われる。次に、端末3から送信してきたユーザID、パスワードからデータベース2を参照してユーザ認証が行われる。認証に成功すれば、D H C P サーバ1はユーザに対応したアクセス制御をルータ4へ依頼するためにC o n f i g u r e - R e q u e s t を送信する（ステップ24）。認証に失敗したならば、クライアントへD H C P N A K を送信する。

【0025】D H C P サーバ1から送信されるC o n f i g u r e - R e q u e s t には、アクセリスト、端末3のMACアドレス、割り当て予定のIPアドレスといった情報が含まれる。

【0026】ルータ4は、D H C P サーバ1から依頼されたアクセリストに基づき、適当なパケットフィルタの設定を行う（ステップ25）。設定が完了したら、ル

7
ータ4はConfigure-AckをDHCPサーバ1へ送信する(ステップ26)。ルータ4から、アクセス制御の設定完了のConfigure-Ackを受信したら、DHCPサーバ1は端末3に対してDHCPACKを送信する(ステップ27)。以上で、ユーザ認証を経て、ネットワークを接続するための必要最低限の設定すなわち初期化が完了となる(ステップ28)。

【0027】この時点で、端末3は、ユーザ認証を経て、最低限の設定情報として、IPアドレス、サブネットマスク、ルーティング情報(デフォルトルート)、IPアドレスのリース時間が既に設定されており、ルータにはアクセリストの設定が行われている。

【0028】次に、端末3(DHCPクライアント)とそれと別サブネット7上に存在するサーバa5間のデータ通信の流れを追いながら、アクセス制御がどのように実現されているのかを説明する。

【0029】端末3は、ルーティングテーブルに基づき、サーバa5宛てのパケットをルータへ送信する。それを受信したルータ4は、ルーティングテーブルに基づき、そのパケットをサーバa5へ転送する。こうしてサーバa5は、端末3から送信されたパケットを受信することができる。逆に、サーバa5から端末3宛のパケットは、そのルーティングテーブルに基づき、ルータ4へ送られる。それを受信したルータ4は、そのルーティングテーブルに基づき、端末3へパケットを転送する。こうして端末3は、サーバa5から送信されたパケットを受信することができる。

【0030】上述のように、端末3から送信されるすべてのパケットは必ずルータ4を経由することになる。つまり、ルータ4は送信パケットが許可されたものであれば転送し、不許可ならば転送せずにパケットを廃棄し、その旨のログ情報を残す。それゆえ、ルータ4はステップ25で設定したアクセリストに基づいて、アクセス制御が可能となる。

【0031】最後に、端末3がすべての処理を終了して、ネットワークから切り離される際に、IPアドレスを開放する手順を図3を用いて説明する。

【0032】端末3は、DHCPサーバ1に対してDHCPRELEASEを送信する(ステップ31)。このメッセージには、ユーザID、パスワードオプションが含まれる。DHCPRELEASEを受信したDHCPサーバ1は、そのメッセージに含まれるユーザID、パスワードからデータベース2に基づいて認証を行なう(ステップ32)。認証に成功すれば、ユーザに対応したアクセス制御の解除をルータ4へ依頼する。そのため、DHCPサーバ1はTerminate-Requestをルータ4へ送信する(ステップ33)。Terminate-Requestを受信したルータ4は、DHCPサーバ1から依頼されたアクセリストに基づき設定を解除し、Terminate-AckをDHCP

10

20

30

40

50

8
Pサーバへ送信する(ステップ34)。

【0033】次に本発明の第2の実施例について図面を参照して詳細に説明する。図4によると、本実施例は、端末3と物理的に同一のサブネット6上にあるサーバb8に対するアクセス制御という点が先の実施例と異なる。

【0034】端末3は、図2の手順で、ユーザ認証を経て、DHCPサーバ1が割り当てる最低限の設定情報として、IPアドレス、サブネットマスク(255.255.255.251)、ルーティング情報(デフォルトルート)、IPアドレスのリース時間が割り当たられる。さらに、最初の実施例では実施されなかった端末3自身のARP Replyの停止が追加実行される。

【0035】ルータ4には、アクセリストの設定、端末3に対するProxy ARPの設定、端末3のMACアドレスのARPテーブルへの登録が図2のステップ25の時点で行われる。Proxy ARPとは、端末3のIPアドレスのARP Requestに対して、ルータ4が代わりにARP Replyを応答するものである。

【0036】ここで特徴的なのは、サブネットマスクとして255.255.255.251、30ビットマスクを使用していることである。この設定により、図4に示すように、ルータ4と端末3は、所属端末が2つのみのサブネット9を形成することになる。そのためサーバb8は、たとえ物理的には同一サブネットに存在しても、論理的に別サブネット上に存在していることになり、サーバb8宛てのパケットはルータ4を経由して送信される。

【0037】次にサーバb8と端末3の通信手順を図5、図6を参照して詳細に説明する。

【0038】図5によれば、まず、端末3はARP Requestをブロードキャストして、ルータ4のMACアドレスを問い合わせる(ステップ40)。ARP Requestを受信したルータ4は、ARP Replyで応答する(ステップ41)。ルータ4のMACアドレスを解決した端末3は、ルータ4へサーバb8宛てのパケットを送信する(ステップ42)。それを受信したルータ4は、ルーティングを行い、パケットをサーバb8へ転送しようとする。(ステップ43)。そこで、ルータ4はARP Requestをブロードキャストして、サーバb8のMACアドレスを解決しようとする(ステップ44)。それに対してサーバb8はARP Replyで応答する(ステップ45)。それを受信したルータ4は、サーバb8へサーバb8宛てのパケットを転送する(ステップ46)。このとき、サーバb6宛てのパケットはルータ4を経由している。

【0039】逆に、サーバb8から端末3宛てのパケットの送信の手順を説明する。図6によれば、サーバb8は、ARP Requestをブロードキャストして、

端末3のMACアドレスを解決しようとする(ステップ50)。それに対して、Proxy ARPの設定がされている(ステップ51)ルータ4は、ARP Replyに自身のMACアドレスを入れて応答する(ステップ52)。一方、端末3は、ARP Reply停止53を行っているので、このARP Requestには応答することができない。アドレス解決をしたサーバb8は、ルータ4へ端末3宛てのパケットを送信する(ステップ54)。それを受信したルータ4は、ルーティングを行い(ステップ55)、端末3へ端末3宛てのパケットを転送する(ステップ56)。このとき、ARPテーブルには端末3のIPアドレスとMACアドレスの組が登録されているので、ARPを使うことなく、ユニキャストでパケットを転送することができる。

【0040】いずれの場合も、端末3から送信されるすべてパケットは、必ずルータ4を経由することになるので、ルータ4のアクセリストによりアクセス制御が可能となる。

【0041】以上、サーバが端末3と同一サブネット6に存在する場合のアクセス制御方法を説明したが、サーバが端末3と同一サブネット6と別サブネット7に同時に存在する場合でも、本実施例と同様にアクセス制御が可能である。

【0042】次に本発明の第3の実施例について図面を参照して詳細に説明する。図7によると、本実施例は、Ethernet上に流れるARP Replyパケットをキャプチャーし、IPアドレスとMACアドレスの組をデータベースに保持する機能を持つエージェント70が存在する点が異なる。

【0043】本実施例では、先の実施例を運用中に、何らかの方法でIPアドレスを不正入手し、手動設定を行うことによりネットワークに端末に接続した場合の対策方法について説明する。

【0044】図8において、エージェント70は、Ethernet上に流れるARP ReplyパケットをキャプチャーしてIPアドレスとMACアドレスの組を収集し、それをデータベース80に保持する。

【0045】一方、DHCPサーバ1が持つデータベース2には、現在アドレスが割り当てられているユーザIDとそのユーザに割り当てたIPアドレス、ユーザの使用している端末のMACアドレス、IPアドレスを割り当てた時刻、リース時間などを含む。

【0046】DHCP以外の手順で正規にIPアドレスを割り当てられた端末の情報を加えたキャッシュデータ2と、エージェントのデータベース80とを定期的に比較検証する。もし、不正に入手したIPアドレスを使用していた端末が存在すると、キャッシュデータにはその端末の情報が存在しないため、上記の比較検証によって不正接続を検出することができる。

【0047】本実施例では、エージェントの導入によ

り、IPアドレスの不正入手による接続を検出できるという新たな効果を有する。

【0048】

【発明の効果】第1の効果は、ユーザ及び端末毎にネットワーク接続可否を制御することができるることにある。

【0049】その理由は、DHCPにユーザ認証を導入したからである。

【0050】第2の効果は、ユーザ及び端末毎にアプリケーションサーバへのアクセス制御を行うことができる

10 ことにある。

【0051】その理由は、DHCPサーバとルータが連携してパケットフィルタを設定し、さらに端末から送信されるすべてのパケットがルータを通過するようにしたためである。

【0052】第3の効果は、ネットワークのIPアドレスを不正入手し、手動設定を行うことによりネットワーク接続した端末を検出することができるることにある。

【0053】その理由は、IPアドレスとMACアドレスの組を収集する機能を持つエージェントを導入したためである。

【0054】第4の効果は、サーバ個別のアクセス制御を不要とすることである。

【0055】その理由は、端末の接続段階でアクセス制御を行い、端末からサーバ宛てのパケットが一切届かないからである。

【図面の簡単な説明】

【図1】第1の実施例の構成を示すネットワーク図である。

【図2】第1の実施例の動作を示すシーケンス図である。

【図3】第1の実施例の動作を示すシーケンス図である。

【図4】第2の実施例の構成を示すネットワーク図である。

【図5】第2の実施例の動作を示すシーケンス図である。

【図6】第2の実施例の動作を示すシーケンス図である。

【図7】第3の実施例の構成を示すネットワーク図である。

【図8】第3の実施例の動作を示す図である。

【符号の説明】

1 DHCPサーバ

2 データベース

3 端末 (DHCPクライアント)

4 ルータ

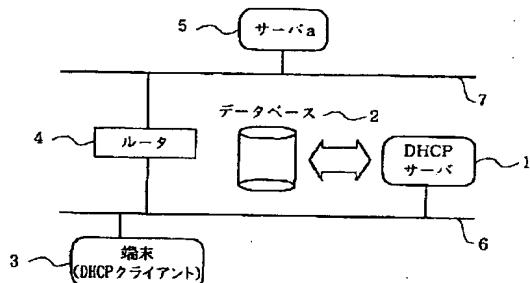
5 サーバa

6、7、9 サブネット

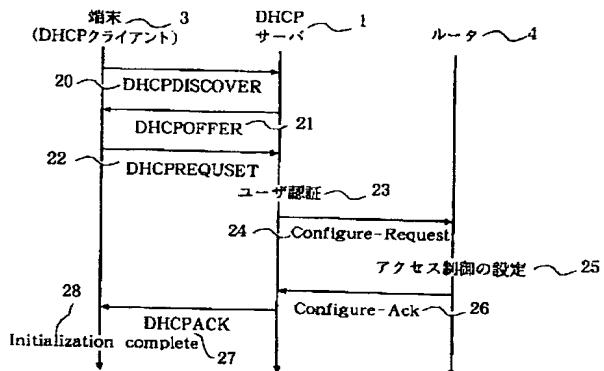
8 サーバb

50 70 エージェント

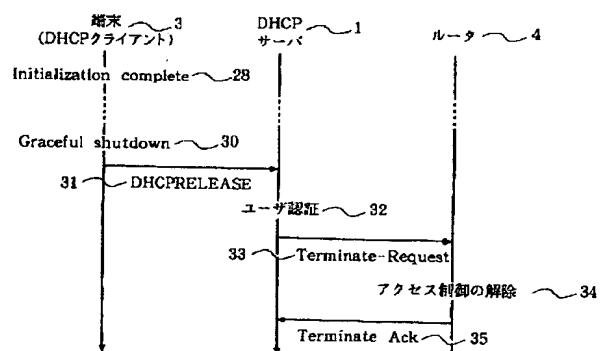
【図 1】



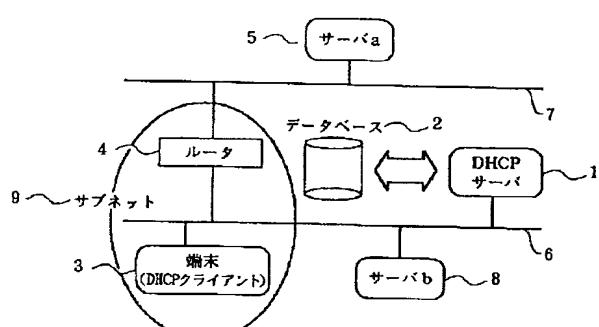
【図 2】



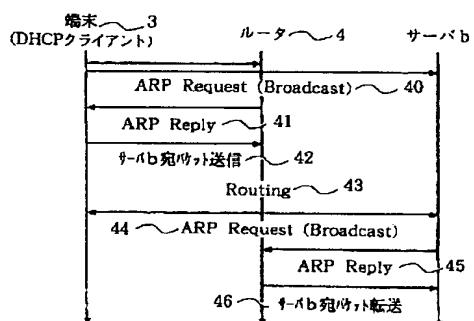
【図 3】



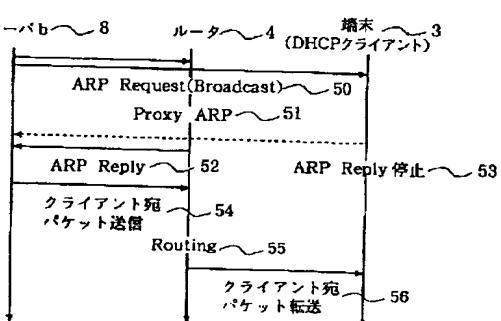
【図 4】



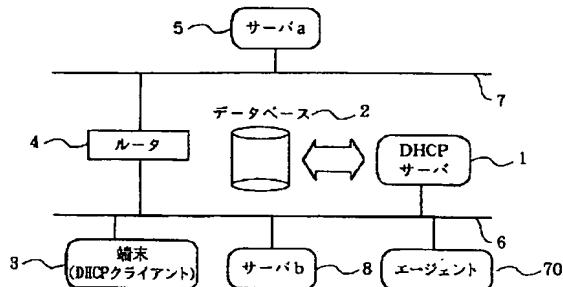
【図 5】



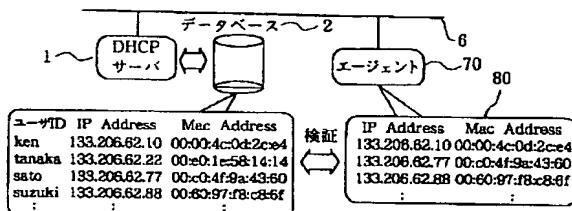
【図 6】



【図 7】



【図 8】



フロントページの続き

F ターム(参考) 5B089 GA11 GA21 GA31 HA01 HA06
 HA10 HB18 JB00 KB06 KB13
 KC58 MB01
 5K030 GA15 HA08 HC14 HD03 HD07
 HD09 JT03 JT06 KA05 LB02
 LC13 LD19 LD20 MD09
 5K033 AA08 CB01 CB08 CC01 DA01
 DA05 DB19 DB20 EA07 EC03

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.